

RECEIVED
CENTRAL FAX CENTER

REMARKS

SEP 14 2006

Reconsideration of the application is requested.

Claims 1-21 remain in the application. Claims 1-21 are subject to examination. Claims 1 and 20 have been amended.

Under the heading "Claim Objections" on page 3 of the above-identified Office Action, the Examiner objected to claims 1 and 20 because of informalities. The Examiner's suggested corrections for claims 1 and 20 have been made.

Under the headings "Response to Arguments" and "Claim Rejections - 35 USC § 102" on pages 2-7 of the above-identified Office Action, claims 1-6, 13-16 and 21 have been rejected as being fully anticipated by U.S. Patent No. 5,757,918 to Hopkins (hereinafter Hopkins) under 35 U.S.C. § 102.

In the Office Action, the Examiner believes that Applicants' arguments were not supported in the claim language. The features that are lacking according to the Examiner concern the direction of transmission, the encryption and the symmetric cryptography.

First, regarding the direction of transmission the following comments are made. In step a) of claim 1 of the instant

- Page 14 of 20 -

application, the data set is communicated so that it is present in an unencrypted form at both the proving and verifying units. The data set is used later in steps f) to i) in a symmetric encryption algorithm. In a symmetric encryption algorithm the direction of transmission for an authentication depends on which side the data has (is on) that is to be confirmed. In principle a challenge and response method for authentication can be initiated from both sides, as both sides have access to the same shared key and the data set. Distinct from this is the use of a public - private key algorithm used in steps b) to f), in which the direction of transmission matters, since the keys on each side are not the same. It is believed that the Examiner mixes the data transmissions of the data set in step a) which is used in steps f) to i) in a symmetric encryption algorithm with the data transmission of the encrypted data element in the public - private key algorithm used in steps b) to f) in order to broaden the claim. However, it is respectfully stated that steps b) to f) are quite clear about the direction of transmission, and therefore we believe the Examiner's arguments are not persuasive as the direction of transmission is inherently defined by the steps themselves.

Second, the following comments are provided regarding the use of a symmetric algorithm. A symmetrical encryption algorithm is characterized by a secret key that is shared between two

entities. Clearly this is the case in claim 1. The verifying unit generates a data element and encrypts it using a public key of the proving unit (in steps b) to f)) before sending it to the proving unit. The encrypted data element can only be decrypted by using a private key of the proving unit and is therefore secret. After the decryption of the encrypted data element in step e) the data element is known only to the verifying unit and the proving unit. It is therefore a shared secret key, which is used in steps f) to i) as a key to authenticate the data set by a challenge and response method. A person of average skill in the art would therefore always consider claim 1 to be using a symmetrical encryption algorithm in steps f) to h), even if it is not explicitly stated in claim 1, because it is inherent in the steps performed.

Third, the following comments are made regarding the encrypted/unencrypted transmission. Again, it is respectfully stated that the Examiner may be mixing up different parts of claim 1 as described above in order to broaden the claim. However, the steps are believed to be quite clear about which data is transmitted encrypted and which unencrypted, and therefore we respectfully disagree with the Examiner's statements.

The Examiner purports that the subject matter of claim 1 is

anticipated by Hopkins. However, we believe that there are considerable differences between the invention of the instant application and Hopkins and now describe some of the critical differences.

In item 6, the Examiner tries to apply Hopkins to step a) of claim 1 and cites column 3, lines 13-14 of Hopkins. However, the cited information fails to disclose anything about an unencrypted data set that is communicated between the proving and verifying unit. It is not clear to which data set the Examiner is referring too. The PIN referred to in the following lines is not stored in the clear in the card (see column 7, line 44) and does not qualify as unencrypted. The value aB is not found in the verifying terminal (see Figs. 2 to 5). At least because of this feature claim 1 of the instant application is novel over Hopkins and therefore cannot be anticipated by Hopkins.

In item 6, the Examiner further tries to apply Hopkins to step c) of claim 1 and cites column 4, lines 39-40. However, the context of the cited lines refers to the communication of the remote facility 22 with the secure facility 20 over the network communications link 26, as shown in Fig. 1 (see column 4, lines 34 - 43). This communications link 26 is not the one referred to by the Examiner in his argument regarding step a) and later steps f) to i) which uses the industry-standard

connectors 25 to connect the smart card 12 to the terminal 24. Because of the Examiner's contradiction and since Hopkins fails to teach one interface having all the features of claim 1, Hopkins cannot anticipate claim 1.

The above is also true where the Examiner tries to apply Hopkins to step d).

Regarding step e), the Examiner is believed to be applying the citation of column 3, lines 27-28 of Hopkins to equate the PIN with the private key known only to the proving unit. However, column 3, lines 16 to 18, teaches that the PIN is entered. From common experience it is known that the PIN is usually entered into the terminal (ATM). Support for this is also found in column 6, lines 8 to 10. As a consequence the PIN is known to the verifying unit and cannot be considered to be a private key known only to the proving unit. Hopkins thus fails to teach step e) and therefore claim 1 is believed to be novel over Hopkins.

Under the heading "Claim Rejections - 35 USC § 103" on pages 7-11 of the above-identified Office Action, claims 7-12 and 17-20 have been rejected as being obvious over Hopkins in view of U.S. Patent No. 5,272,755 to Miyaji et al. (hereinafter Miyaji) under 35 U.S.C. § 103.

Claims 7-12 and 17-20 ultimately depend on claim 1. Because claim 1 is believed to be allowable, claims 7-12 and 17-20 are also believed to be allowable.

It is accordingly believed to be clear that none of the references, whether taken alone or in any combination, either show or suggest the features of claim 1. Claim 1 is, therefore, believed to be patentable over the art. The dependent claims are believed to be patentable as well because they all are ultimately dependent on claim 1.

In view of the foregoing, reconsideration and allowance of claims 1-21 are solicited.

If an extension of time is required, petition for extension is herewith made. Any extension fee associated therewith should be charged to the Deposit Account of Lerner Greenberg Stemer, LLP, No. 12-1099.

Please charge any other fees that might be due with respect to Sections 1.16 and 1.17 to the Deposit Account of Lerner

Greenberg Steiner LLP, No. 12-1099.

Respectfully submitted,

Ralph E. Lerner
Registration No. 41,947

September 14, 2006

Lerner Greenberg Steiner LLP
P.O. Box 2480
Hollywood, Florida 33022-2480
Tel.: (954) 925-1100
Fax: (954) 925-1101